

SYSTEM AND METHOD FOR ENHANCED PIRACY PROTECTION IN A  
WIRELESS PERSONAL COMMUNICATION DEVICE

5

Abstract of the Disclosure

A key-sharing scheme is used to control distribution and use of video and  
audio content in personal digital assistants (PDAs) and other wireless devices. A  
10 private key is split into key-shares using a Blakley-Shamir key splitting technique  
and the key-shares are distributed to various network entities including a finance  
server and security server. Key-shares are also stored in a user's subscriber  
identity module (SIM) and a security processor of the PDA. The key-shares from  
the network entities are provided to the PDA after the user requests specific video  
15 or audio content and a credit verification is performed. The PDA's security  
processor combines the key-shares to form the decryption key for use in playing  
the content by the PDA's communications processor. When a service limit is  
reached, the PDA's security processor purges the key-shares to prevent further use  
of the content.

"Express Mail" mailing label number: EL806497320US

Date of Deposit: July 31, 2001

This paper or fee is being deposited on the date indicated above with  
the United States Postal Service pursuant to 37 CFR 1.10, and is  
addressed to the Commissioner for Patents, Box Patent Application,  
Washington, D.C. 20231.